WHAT IS CLAIMED IS:

1. A method of integrating telephony function with security and guidance features on an Internet appliance comprising the steps of:

selecting a communication access number using a selection means, said communication access number operable to access a communication link via said Internet appliance;

alerting a user of said Internet appliance when an attempt is made to select said communication link via a dialing action of said Internet appliance using said communication access number; and

receiving an authorization for said dialing action by said user of said Internet appliance.

2. The method of claim 1 wherein said authorization comprises the sub steps of:

prompting said user to enter a user personal identification means (PIM) in response to selecting said communication access number;

initiating a pre-determined security protocol to retrieve a corresponding secure PIM for comparison;

correlating said user personal identification means with said secure PIM;

authorizing or rejecting said dialing action in response to said correlation;

retrieving secure device driver code for executing said dialing action using said security protocol in response to said authorization;

displaying, if said dialing action is authorized, a connectivity cost alert for said communication link; and

executing said dialing action using said device driver code for said communication link in response to said authorization and a user response to said connectivity cost alert.

3. The method of claim 1, further comprising the step of:

using said security protocol for encrypting and decrypting information transmitted on said communication link in response to authorizing said dialing action for said communication link.

4. The method of claim 1, wherein said security protocol is a Public/Private key encryption protocol.

5. The method of claim 1, wherein said PIM is used to grant or block access to certain area or country telephony codes.

6. The method of claim 1, further comprising the step of:

matching said communication access number with an actual system entered communication access number.

7. The method of claim 1, further comprising the steps of:

monitoring an incoming call for a caller ID; and

answering and routing said incoming call to a receiving device on the basis of said incoming telephone number.

8. The method of claim 1, further comprising the step of:

using a built-in key escrow function to notify a trusted server of a current dynamic host configuration protocol (DHCP) assigned IP address along with a key indicating authenticity of transmission so that voice over IP services between devices and a web page server lookup may be performed in a DHCP environment without side-channel communication for call or web reference look-up.

9. The method of claim 1, wherein activating said selected communication access number comprises selecting said communication access number from a displayed Internet web page hot spot.

10. The method of claim 1, wherein said communication access number is selected using an actual or virtual keypad of said Internet appliance.

11. The method of claim 1, wherein said communication link comprises a non-concurrent shared dial-up public switched telephone network (PSTN) connection between a telephone connection and an Internet connection.

12. The method of claim 1, wherein said communication link has separate connections for an Internet connection and a telephone connection.

13. The method of claim 1, wherein said communication link comprises a concurrent communication link for an Internet and a telephone connection.

14. A system for integrating telephony function with security and guidance features on an Internet appliance (IA):

one or more personal identification means (PIM) input units coupled to a system bus in said ICA, said PIM input units operable to generate unique PIM signals;

a security protocol circuit operable to encrypt, decrypt, store and retrieve said PIM signals and device driver code;

a PIM verification circuit operable to receive said PIM signals and compare them to secure predetermined PIM signals, said PIM verification circuit generating a verification signal;

one or more Modems coupled to a dialing action controller and to communication lines; said Modems operable to send and receive communication data; and

a dialing action controller (DAC) coupled to said system bus and said Modems, said DAC operable receive a dialing action request and to alert a user of said dialing action and to enable or disable said dialing action to said Modems in response to said verification signal and a user signal.

15. The system of claim 13, wherein said authorization unit comprises:

a smart card reader;

a biometric input unit;

a personal identification number input unit; and

a voice recognition input unit,

16. The system of claim 13, wherein said Modem comprises:

a digital subscriber line (DSL) Modem;

17. The system of claim 13, wherein said Modem comprises:
a wireless cellular modem;

18. The system of claim 13, wherein said Modem comprises:
a wireless personal communication system (PCS) modem;

19. The system of claim 13, wherein said Modem comprises:
a cable Modem.

20. The system of claim 13, wherein said Modem comprises a public subscriber telephone network (PSTN) Modem.

21. The system of claim 13, wherein said DAC alerts said user of a dialing action by display on a user display screen coupled to said IA.

22. The system of claim 13, wherein said DAC retrieves a connectivity cost and alerts said user of a connectivity cost associated with a requested dialing action if said dialing action is authorized.

23. The system of claim 13, wherein said user signal is a response by said user to said connectivity cost alert for said dialing action.

24. The system of claim 13, wherein said user is given an option of communicating on an established communication link in response to an authorized and enabled dialing action using said security protocol.

25. The system of claim 13, wherein said DAC uses a built-in key escrow function to notify a trusted server of a current dynamic host configuration protocol (DHCP) assigned IP address along with a key indicating authenticity of transmission so that voice over IP services between devices and a web page server lookup may be performed in a DHCP environment without side-channel communication for call or web reference look-up.

26. The system of claim 13, wherein said dialing action request comprises:

entering a communication access number via a keyboard keypad, a virtual display keypad, or by clicking a "hot spot" on a Web page.

27. The system of claim 13, wherein said connectivity cost alert notifies a user of an actual toll call cost for a communication link corresponding to said authorized and enabled dialing action.

28. The system of claim 13, wherein said user is alerted of said dialing action whether said dialing action was initiated locally or remote by another user.

29. The system of claim 13, wherein DAC monitors incoming communication access numbers and directs communication to a answering or recording device or forwards the communication to another communication link in response to comparing said incoming communication access numbers to a predetermined, stored communication access numbers list.

30. An Internet appliance, comprising:

a central processing unit (CPU);

a read only memory (ROM);

a random access memory (RAM);

a user interface adapter coupled to a keyboard and a mouse;

a display interface adapter coupled to a user display;

an I/O interface adapter;

a system bus;

a communication adapter; and

a security processor unit,

said security processor unit further comprising:

one or more personal identification means (PIM) input units coupled to a system bus in said ICA, said PIM input units operable to generate unique PIM signals;

a security protocol circuit operable to encrypt, decrypt, store and retrieve said PIM signals and device driver code;

a PIM verification circuit, said PIM verification circuit operable to receive said PIM signals and compare them to secure predetermined PIM signals, said PIM verification circuit generating a verification signal;

one or more Modems coupled to a dialing action controller and to communication lines, said Modems operable to send and receive communication data; and

a dialing action controller (DAC) coupled to said system bus and said Modems, said DAC operable receive a dialing action request and to alert a user of said dialing action and to enable or disable said dialing

action to said Modems in response to said verification signal and a user signal.

31. The Internet appliance of claim 29, wherein said PIM input unit comprises:
a smart card reader;
a biometric input unit;
a personal identification number input unit; and
a voice recognition input unit

32. The Internet appliance of claim 29, wherein said Modem comprises:
a digital subscriber line (DSL) Modem.

33. The Internet appliance of claim 29, wherein said Modem comprises:
a wireless cellular modem.

34. The Internet appliance of claim 29, wherein said Modem comprises:
a wireless personal communication system (PCS) modem.

35. The Internet appliance of claim 29, wherein said Modem comprises
a cable Modem.

36. The Internet appliance of claim 29, wherein said Modem comprises a public subscriber telephone network (PSTN) Modem.

37. The Internet appliance of claim 29, wherein said DAC alerts said user of a dialing action by display on a user display screen coupled to said IA.

38. The Internet appliance of claim 29, wherein said DAC retrieves a connectivity cost and alerts said user of a connectivity cost associated with a requested dialing action if said dialing action is authorized.

39. The Internet appliance of claim 29, wherein said user signal is a response by said user to said connectivity cost alert for said dialing action.

40. The Internet appliance of claim 29, wherein said user is given an option of communicating on an established communication link in response to an authorized and enabled dialing action using data encryption.

41. The Internet appliance of claim 29, wherein said DAC uses a built-in key escrow function to notify a trusted server of a current dynamic host configuration protocol (DHCP) assigned IP address along with a key indicating authenticity of transmission so that voice over IP services between devices and a web page server lookup may be performed in a DHCP environment without side-channel communication for call or web reference look-up.

42. The Internet appliance of claim 29, wherein said dialing action request comprises:

entering a communication access number via a keyboard keypad, a virtual display keypad, or by clicking a "hot spot" on a Web page.

43. The Internet appliance of claim 29, wherein said connectivity cost alert notifies a user of an actual toll call cost for a communication link corresponding to said authorized and enabled dialing action.

44. The Internet appliance of claim 29, wherein said user is alerted of said dialing action whether said dialing action was initiated locally or remote by another user.

45. The Internet appliance of claim 29, wherein DAC monitors incoming communication access numbers and directs communication to a answering or recording device or forwards the communication to another communication link in response to comparing said incoming communication access numbers to a predetermined, stored communication access numbers list.